U.S. DEPARTMENT OF COMMERCE PATENT & TRADEMARK OFFICE

B/O Form PTO-1390 **Transmittal Letter to the United States Designated/Elected Office (DO/EO/US) Concerning a Filing Under *35 USC 371***		*Attorney's Docket Number* JEK/Vedder
		U S Application Number (if known) 09/673658
International Application Number PCT/EP99/02848	*International Filing Date* 27 April 1999	*Priority Date Claimed* 07 May 1998
Title of Invention METHOD FOR AUTHENTICATING A CHIP CARD IN A MESSAGE TRANSMISSION NETWORK		
Applicant(s) for DO/EO/US Klaus VEDDER		

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items under *35 USC 371*:

1. ☒ This is a **FIRST** submission of items concerning a filing under *35 USC 371*.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under *35 USC 371*.
3. ☒ This express request to begin national examination procedures *(35 USC 371(f))* at any time rather than delay examination until the expiration of the applicable time limit set in *35 USC 371(b)* and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed *35 USC 371(c)(2)*.
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ A translation of the International Application into English *(35 USC 371(c)(2))*.
7. ☒ Amendments to the claims of the International Application under PCT Article 19 *(35 USC 371(c)(3))*
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 *(35 USC 371(c)(3))*.
9. ☒ An oath or declaration of the inventor(s) *(35 USC 371(c)(4))*. (☐ Executed ☒ Unexecuted)
10. ☒ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 *(35 USC 371(c)(5))*.

Items 11 to 16 below concern other document(s) or information included:

11. ☐ An Information Disclosure Statement under *37 CFR 1.97* and *1.98*.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with *37 CFR 3.28* and *3.31* is included.
13. ☒ A **FIRST** preliminary amendment.
    ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: 2 sheets formal drawings

Application Number (if known) 09/673658	International Application Number PCT/EP99/02848	Attorney's Docket Number JEK/Vedder	
		Calculations	PTO USE ONLY

17. The following fees are submitted:

Basic National Fee *(37 CFR 1.492(a)(1)-(5))*:

- ☒ Search report has been prepared by the EPO or JPO $860.00
- ☐ International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)* $690.00
- ☐ No International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)* but International Search Fee paid to USPTO *(37 CFR 1.445(a)(2))* $710.00
- ☐ Neither International Preliminary Examination Fee *(37 CFR 1.482)* nor International Search Fee *(37 CFR 1.445(a)(2))* paid to USPTO $1000.00
- ☐ International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)* and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00

ENTER APPROPRIATE BASIC FEE AMOUNT					**$ 860.00**	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date *(37 CFR 1.492(e))*.						
CLAIMS	NUMBER FILED		NUMBER EXTRA	RATE		
Total Claims	11	-20 =		× $18.00		
Independent Claims	1	-3 =		× $80.00		
Multiple Dependent Claims (if applicable)				+ $270.00		
TOTAL OF ABOVE CALCULATIONS					**$ 860.00**	
Reduction by ½ for filing by small entity, if applicable. Verified Small Entity Statements must also be filed (Note *37 CFR 1.9, 1.27, 1.28)*						
SUBTOTAL					**$ 860.00**	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date *(37 CFR 1.492(f))*.						
TOTAL NATIONAL FEE					**$ 860.00**	
Fee for recording the enclosed assignment *(37 CFR 1.21(h))*. The assignment must be accompanied by an appropriate cover sheet *(37 CFR 3.28, 3.31)*. **$40.00** per property.						
TOTAL FEES ENCLOSED					**$ 860.00**	
				Amount to be:	Refunded:	
					Charged:	

a. ☒ A check in the amount of **$860.00** to cover the fees is enclosed.

b. ☐ Please charge my **Deposit Account Number 02-0200** in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to **Deposit Account Number 02-0200**. A duplicate copy of this sheet is enclosed.

Note: Where an appropriate time limit under *37 CFR 1.494* or *1.495* has not been met, a petition to revive *(37 CFR 1.137(a) or (b))* must be filed and granted to restore the application to pending status.

BACON & THOMAS, PLLC
625 SLATERS LANE - FOURTH FLOOR
ALEXANDRIA, VIRGINIA 223124-1176
(703) 683-0500

DATE: 06 November 2000

Respectfully submitted,

J. ERNEST KENNEY
Attorney for Applicant
Registration Number: 19,179

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

International Patent Application
No. PCT/EP99/02848

PCT/DO/EO/US

International Filing Date: 27 April 1999

Applicant: Klaus VEDDER

For: METHOD FOR AUTHENTICATING A CHIP CARD IN A MESSAGE TRANSMISSION NETWORK

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

This paper accompanies documents submitted to establish the U.S. national stage of the above-identified international patent application.

The international patent application was amended under PCT Article 34 and the claims as-amended are annexed to the International Preliminary Examination Report (IPER).

Before calculation of the filing fee and before examination, kindly amend the claims as annexed to the IPER as follows:

IN THE CLAIMS:

Claim 3, line 1; delete "or 2";

Claim 4, line 1; change "any of claims 1 to 3" to --claim 1--;

Claim 5, line 1; change "any of claims 1 to 4" to --claim 1--;

Claim 6, line 1; change "any of claims 1 to 5" to --claim 1--;

Claim 7, line 1; change "any of claims 1 to 5" to --claim 1--;

Claim 8, line 1; change "any of claims 1 to 5" to --claim 1--;

Claim 9, line 1; change "any of claims 1 to 8" to --claim 1--;

Claim 10, line 1; change "any of claims 1 to 9" to --claim 1--;

Claim 11, line 1; change "any of claims 1 to 10" to --claim 1--;

REMARKS

All rights are reserved to the original claimed subject matter. The claims have been amended to reduce the filing fees and to correct any improper multiple dependent claims. Examination of the application as amended is respectfully requested.

Respectfully submitted,
BACON & THOMAS, PLLC

J. ERNEST KENNEY
Attorney for Applicant
Registration Number 19,179

BACON & THOMAS, PLLC
625 Slaters Lane, Fourth Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500
Facsimile: (703) 683-1080

Date: November 5, 2000

S:\Producer\jek\VEDDER - pct02848\preliminary amendment.wpd

Method for authenticating a smart card within a messaging network

This invention relates to a method for authenticating a smart card in a messaging network, preferably a GSM network, according to the preamble of claim 1.

In GSM systems it is known that for using the smart card (subscriber identity module, SIM) the user must usually first identify himself as an authorized user by means of a personal identification number (PIN). In order to avoid abuse at this point, it is known to provide an error counter for the PIN entry to prevent further use of the card after a permissible number of failed attempts is exceeded.

A further system-relevant security measure is to authenticate the card vis-à-vis the mobile network. A secret key inaccessible from outside and an algorithm likewise inaccessible from outside are stored in the card. For authentication a random number is generated by the network or a network component and transferred to the card. The card then calculates from the random number and secret key by means of the algorithm present in the card a response which it transfers to the network. This response is analyzed in the network and, if the result is positive, access to the network functions is allowed. The corresponding procedure is described in the relevant GSM specifications.

A network protected as stated above involves the danger that attacks on the algorithm used for authentication permit the network to be simulated in a computer for example by e.g. selected "random numbers" being transmitted to the SIM card according to the standardized protocol and the secret key of the smart card being determined therefrom, after several authentication attempts. If the algorithm of the card is additionally known, essential functional elements of the card can be simulated or duplicated after determination of the secret key.

It is therefore the problem of the invention to state a reliable method for authenticating a smart card in a messaging system wherein there is no acknowledgment of the authentication result to the subscribing smart card, as customary in the GSM network for example.

This problem is solved according to the invention starting out from the features of the preamble of claim 1 by the characterizing features of claim 1.

Advantageous embodiments of the invention are stated in the dependent claims.

The invention provides for forming the authentication message by forming at least two parts from both the secret key and the random number transferred by the network, one of the parts of the transferred random number and one or more parts of the secret key being encrypted by means of a one- or multistep, preferably symmetrical calculation algorithm. To output an authentication message, a selectable part of the result calculated according to the authentication algorithm is transferred to the network.

An advantageous embodiment of the invention provides for generating the channel coding key in the same way. There too it is provided that, if key and random number are split into two parts for example, either the first or the second part of the transferred random number is linked with the first and/or second part of the secret key with a one- or multistep algorithm in order to obtain a channel coding key. One preferably uses different parts of the random number obtained from the network for forming the authentication message and the channel coding key in each case.

A further advantageous embodiment of the invention provides that the secret key stored in the card and the random number sent by the network to the card are split into equally long parts. This permits the same calculation algorithm to be used in both cases. The random number or secret key can be split by simply making a split "in the middle" or by creating overlapping partial areas. One can also effect a split by which the sum of the individual parts is smaller than the bit length of the random number or secret key. According to a further variant, a given number of bits of the random number or secret key can be combined into a key or random number part according to a predetermined pattern or pseudorandomly.

As a further advantageous embodiment of the invention, one can use DES algorithms as calculation algorithms for authentication and for channel coding.

Another advantageous variant of the invention provides for using the preferably one-step IDEA algorithm for calculating the authentication parameters and channel coding keys.

Alternatively, one can calculate the authentication parameters and channel coding keys using compression algorithms, preferably cryptographic compression algorithms whose output values have a smaller length than the input parameters.

To increase security it is advantageous to use an at least two-step calculation algorithm, whereby a triple DES algorithm proves especially safe. With this algorithm one first encrypts with a first part of the key and a part of the random number, then performs decryption of the result with the second part of the key, and finally executes a further calculation with the first part of the key again. For the last encryption with the first part of the key one can advantageously use a new, third key, in particular if the key is split into three key parts.

A further advantageous embodiment of the invention results if the selection of the first or second part of the random number is effected alternatingly for authentication and calculation of the channel coding, this alternation being executed randomly or pseudorandomly and the selection being effected in the same way in the card and the network.

The invention will be described more closely in the following with reference to Figures 1 to 3.

Fig. 1 shows the sequence of cryptographic functions of the SIM in the GSM network.

Fig. 2 shows a block diagram of triple DES encryption.

Fig. 3 shows examples of the split of the secret key and random number.

The sequence shown in Fig. 1 assumes that the customary, preceding process of PIN verification has been completed. Subsequently, the mobile unit in which card *SIM* is located sends to the network a message which contains IMSI (international mobile subscriber identity) information or TMSI (temporary mobile subscriber identity) information. Secret key K_i is determined from the IMSI or TMSI in the network according to a given function or by means of a table. The same key is also stored in smart card *SIM* in an inaccessible memory space. The secret key is required for later verification of the authentication process.

The network then initiates the authentication process by calculating random number *RAND* and transferring it via the air interface to smart card *SIM*.

Authentication parameter *SRES* is thereupon formed in the smart card by means of an authentication algorithm from secret key K_i and random number *RAND*, said parameter being in turn transferred via the air interface to the network. According to the invention, at least two random numbers $RAND_1$ and $RAND_2$ are derived from random number *RAND*. Random numbers $RAND_1$ and $RAND_2$ can be obtained by division or a selection from random number *RAND* or by a calculation algorithm.

Authentication is effected with a two-step algorithm in the example according to Fig. 1. First, as indicated in Fig. 1, first part $RAND_1$ of the random number is encrypted with first part K_1 of key K_i likewise split into two parts. The result of said first step is subsequently encrypted in a second step with second part K_2 of the key. For calculation with the authentication algorithm one can of course also use second part $RAND_2$ of the random number first and change the order of using first and second key parts K_1 and K_2.

Authentication parameter *SRES'* is meanwhile likewise formed in the network in the same way as in the card by means of the authentication algorithm and random number *RAND* ($RAND_1$, $RAND_2$) and secret key *Ki* (K_1, K_2). Parameter *SRES'* is then compared in the network with authentication parameter *SRES* obtained from the card. If authentication parameters *SRES'* and *SRES* match, the authentication process is completed successfully. If the authentication parameters do not match, the subscriber's card is regarded as unauthenticated. It should be noted here that one can also form *SRES* or *SRES'* using only parts of the result obtained by the encryption.

In the same way as the authentication parameters are generated, key *Kc* for channel coding for data and speech transmission is generated in the card and the network. One preferably uses as the input parameter the part of random number *RAND* not used in authentication.

Figure 2 shows an advantageous example by which calculation with the authentication algorithm and/or channel coding is executed by a triple DES algorithm. According to this algorithm, part $RAND_1$ or $RAND_2$ of the random number is first encrypted with first key part K_1. In the next step decryption is effected with K_2. The result is then encrypted with K_1 again or, if the random number/key is split into

a plurality of parts, with a third part of the key. The channel coding is formed in the same way. The corresponding algorithms are used in the network in each case.

Without restricting universality, the description of the examples according to Figs. 1 and 2 assumed a two- or three-step, symmetrical encryption algorithm. The inventive idea, which consists of splitting the random number and secret key, can of course also be executed with other, common encryption or calculation algorithms. By way of example, mention is made of not only the DES algorithms (A3; A8) but also IDEA. The stated algorithms can also be executed in one step, whereby different parts of the key and/or random number are preferably generated for authentication and generation of channel coding key *Kc*.

Figures 3*a* to *e* give examples of ways of splitting secret key K_i or random number *RAND*.

Figure 3*a* shows key K_i or random number *RAND* with a length of 128 bits.

Figure 3*b* shows a split into two equal parts K_1 and K_2 ($RAND_1$, $RAND_2$), the split being made in the middle. Part 1 contains bit 1 to bit 64, part 2 contains bit 65 to bit 128. Figure 3*c* shows an overlapping split, and Figure 3*d* shows a split by which the odd bits are assigned to part 1 and the even bits to part 2. Figure 3*e* finally shows a split by which the sum of the bit positions of parts 1 and 2 is smaller than the bit positions of the initial key or random number.

New patent claims

1. A method for authenticating a smart card (*SIM*) in a messaging network, preferably a GSM network, wherein an algorithm and a secret key are stored in a smart card (*SIM*), whereby for authentication
   - the network or a network component first transfers a random number (*RAND*) to the smart card,
   - a response signal (*SRES*) is generated therefrom in the smart card by means of the algorithm and the secret key (K_i) and transmitted to the network or network component,

   characterized in that
   - to form the response signal (*SRES*) the secret key (K_i) and the random number (*RAND*) are each split into at least two parts (K_1, K_2; $RAND_1$, $RAND_2$),
   - one of the parts ($RAND_1$, $RAND_2$) of the transferred random number (*RAND*) is encrypted with the aid of one or more parts (K_1, K_2) of the secret key (K_i) by means of a one- or multistep, preferably symmetrical algorithm.
2. A method according to claim 1, characterized in that a given number of bits is selected from the encryption result and transferred as a signal response (*SRES*) to the network.
3. A method according to claim 1 or 2, characterized in that the secret key (K_i) and/or the random number (*RAND*) are split into two parts.
4. A method according to any of claims 1 to 3, characterized in that a part of the transferred random number (*RAND*) and one and/or more parts of the secret key (K_i) are used to calculate a channel coding key (K_c) by means of a one- or multistep algorithm, at least one part of the calculation result being used as the channel coding key (K_c).

5. A method according to any of claims 1 to 4, characterized in that the key (K_i) and the random number (*RAND*) are split into two equally long parts (K_1, K_2/ $RAND_1$, $RAND_2$).
6. A method according to any of claims 1 to 5, characterized in that DES algorithms are used to calculate the authentication parameters (*SRES*, *SRES'*) and/or the channel coding key (K_c).
7. A method according to any of claims 1 to 5, characterized in that the, preferably one-step, IDEA algorithm is used to calculate the authentication parameters (*SRES*, *SRES'*) and/or the channel coding key (K_c).
8. A method according to any of claims 1 to 5, characterized in that a compression algorithm whose output value has a smaller length than the input parameter is used to calculate the authentication parameters (*SRES*, *SRES'*) and/or the channel coding key (K_c).
9. A method according to any of claims 1 to 8, characterized in that the calculation is effected in an at least two-step algorithm.
10. A method according to any of claims 1 to 9, characterized in that a triple DES algorithm is used as an encryption algorithm, whereby one first encrypts with the first part (K_1) of the key (K_i), then decrypts with the second part (K_2) of the key (K_i) and thereupon encrypts again with the first part (K_1) or a third part of the key (K_i).
11. A method according to any of claims 1 to 10, characterized in that a selection of the first or second part of the random number (*RAND*) is effected in the same way in the card and the network in random or pseudorandom alternation.

Abstract

The invention relates to a method for authenticating a smart card (*SIM*) in a messaging network, preferably a GSM network, wherein an optionally secret algorithm and a secret key are stored in a smart card (SIM), whereby for authentication the network or a network component first transfers a random number to the smart card, a response signal is generated in the smart card by means of the algorithm, the random number and the secret key, said signal being transmitted to the network or network component in order to check the authenticity of the card there. According to the invention both the secret key and the random number transferred by the network are split into at least two parts to form the authentication message, one part of the transferred random number and one or more parts of the secret key being encrypted by means of a one- or multistep, preferably symmetrical calculation algorithm. To output an authentication response, a selectable part of the encryption result is transferred to the network.

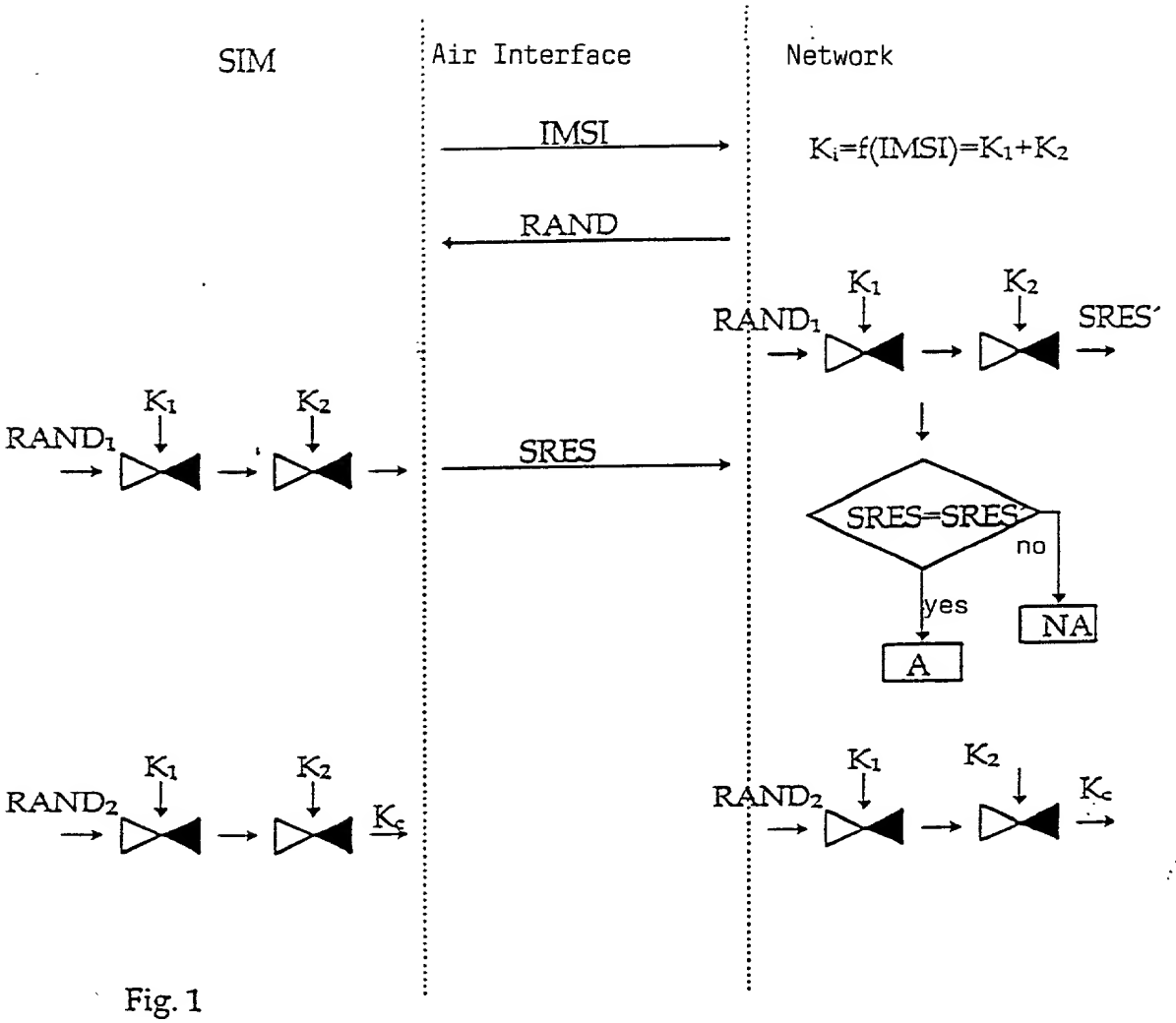

Fig. 1

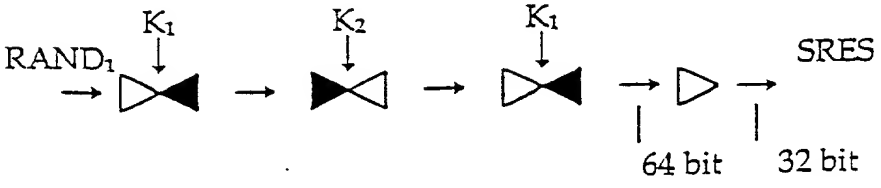

Fig. 2

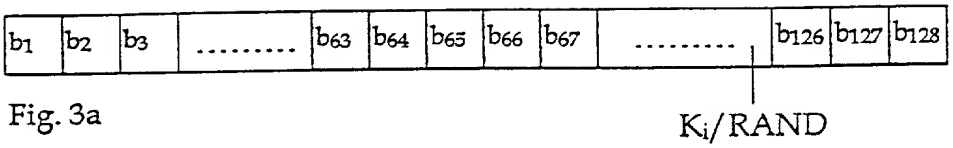

Fig. 3a

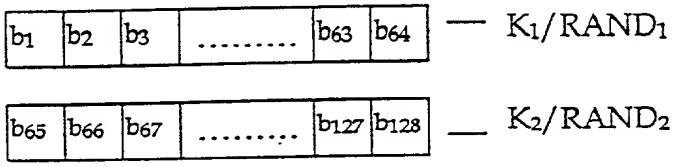

Fig. 3b

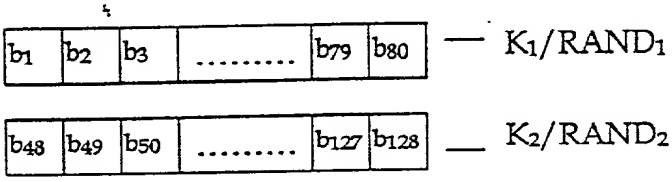

Fig. 3c

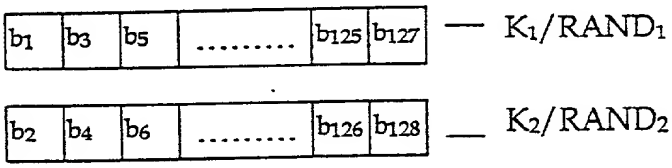

Fig. 3d

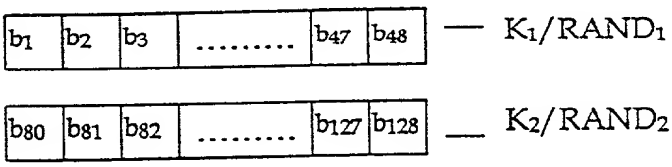

Fig. 3e

ATTORNEY/DOCKET NO: **JEK/Vedder**

DECLARATION FOR PATENT APPLICATION AND APPOINTMENT OF ATTORNEY

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name; I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention (Design, if applicable) entitled:

METHOD FOR AUTHENTICATING A CHIP CARD IN A MESSAGE TRANSMISSION NETWORK

the specification of which (check one):

☐ is attached hereto, or ☒ was filed on: **27 April 1999** as U.S. Application Number or PCT International Application Number: **09/673,658**

and (if applicable) was amended on:

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment(s) referred to above. I acknowledge the duty to disclose information which is material to patentability as defined in *Title 37, Code of Federal Regulations, §1.56*. I hereby claim foreign priority benefits under *Title 35, United States Code §119* of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed.

PRIOR FOREIGN APPLICATION(S)			PRIORITY CLAIMED	
Number	Country	Day/Month/Year Filed	Yes	No
198 20 422.1	Germany	07 May 1998	X	

☐ Additional Priority Application(s) Listed on Following Page(s)

I HEREBY CLAIM THE BENEFIT UNDER TITLE 35 U.S. CODE §119(E) OF ANY U.S. PROVISIONAL APPLICATIONS LISTED BELOW.	
Application Number	Day/Month/Year Filed

☐ Additional Provisional Application(s) Listed on Following Page(s)

I hereby claim the benefit under *Title 35, United States Code, §120* of any United States application(s) or PCT international application(s) designating The United States of America listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of *Title 35, United States Code, §112*, I acknowledge the duty to disclose information which is material to patentability as defined in *Title 37, Code of Federal Regulations, §1.56* which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

Application Number	Filing Date	Status - Patented, Pending or Abandoned

☐ Additional US/PCT Priority Application(s) listed on Following Page(s)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under *section 1001 of title 18 of the United States Code* and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: I (We) hereby appoint as my (our) attorneys, with full powers of substitution and revocation, to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: J. Ernest Kenney, Reg. No. 19,179; Eugene Mar, Reg. No. 25,893; Richard E. Fichter, Reg. No. 26,382; Thomas J. Moore, Reg. No. 28,974; Joseph DeBenedictis, Reg. No. 28,502; Benjamin E. Urcia, Reg. No. 33,805; and

I(we) authorize my(our) attorneys to accept and follow instructions from **Klunker Schmitt-Nilson Hirsch** regarding any matter related to the preparation, examination, grant and maintenance of this application, any continuation, continuation-in-part or divisional based thereon, and any patent resulting therefrom, until I(we) or my(our) assigns withdraw this authorization in writing.

Send correspondence to: **BACON & THOMAS, PLLC**
625 Slaters Lane - 4th Floor
Alexandria, VA 22314-1176

Telephone Calls to: **J. Ernest Kenney (703) 683-0500**

FULL NAME OF FIRST OR SOLE INVENTOR	CITIZENSHIP
Klaus VEDDER	**Germany**
RESIDENCE ADDRESS Ainmillerstrasse 38, 80801 Munchen Germany	POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW
DATE 12/01/2000	SIGNATURE X

☐ *See following page(s) for additional joint inventors.*